ประจำวันพุธที่ 17 สิงหาคม 2565

มัลแวร์ SOVA เพิ่มคุณสมบัติแรนซัมแวร์ เพื่อเข้ารหัสบนอุปกรณ์ Android

โทรจันธนาคาร SOVA Android ยังคงพัฒนาอย่างต่อเนื่องซึ่งเห็นได้จากคุณสมบัติใหม่คือความสามารถในการปรับปรุงโค้ดได้และการเพิ่มคุณสมบัติแรนซัมแวร์ที่เข้ารหัสไฟล์บนอุปกรณ์มือถือ ในเวอร์ชันล่าสุด มัลแวร์ SOVA นั้นมีเป้าหมายโจมตีมากกว่า 200 ธนาคาร การแลกเปลี่ยนสกุลเงินดิจิทัล และแอปพลิเคชันกระเป๋าเงินดิจิทัล โดยมีความพยายามที่จะขโมยข้อมูลผู้ใช้ที่ละเอียดอ่อนและคุกกี้จากพวกเขา ยิ่งไปกว่านั้น มันยังมีฟีเจอร์โค้ดที่ปรับโครงสร้างและปรับปรุงแล้ว ซึ่งช่วยให้ทำงานได้อย่างลับ ๆ มากขึ้นบนอุปกรณ์ที่ถูกบุกรุก ในขณะที่เวอร์ชันล่าสุด 5.0 จะเพิ่มโมดูลแรนซัมแวร์ด้วย

นักวิเคราะห์ภัยคุกคามของบริษัทรักษาความปลอดภัยมือถือ Cleafy ได้ติดตามวิวัฒนาการของ SOVA นับตั้งแต่มีการประกาศโครงการในเดือนกันยายน พ.ศ. 2564 และรายงานว่ามีการพัฒนามากขึ้นอย่างรวดเร็วในปี พ.ศ. 2565 โดยในเดือนมีนาคม พ.ศ. 2565 SOVA ได้เปิดตัวเวอร์ชัน 3 โดยเพิ่มการสกัดกั้น 2FA การขโมยคุกกี้ และการเพิ่มช่องทางใหม่ให้กับธนาคารหลายแห่งทั่วโลก การแทรกเป็นภาพซ้อนทับที่แสดงเหนือข้อความแจ้งการเข้าสู่ระบบที่ถูกต้องซึ่งใช้ในการขโมยข้อมูล ในเดือนกรกฎาคม พ.ศ. 2565 ทีมพัฒนาของ SOVA ได้เปิดตัวเวอร์ชัน 4 ซึ่งใช้แอปเป้าหมายได้มากถึง 200 แอป และเพิ่มความสามารถ VNC (การประมวลผลเครือข่ายเสมือน) สำหรับการฉ้อโกงบนอุปกรณ์ โดยมัลแวร์จะส่งรายการแอปพลิเคชันที่ติดตั้งไปยัง C2 และรับ XM ที่มีรายการที่อยู่ซึ่งชี้ไปยังโอเวอร์เลย์ที่ถูกต้องเพื่อโหลดเมื่อเหยื่อเปิดแอปเป้าหมาย เวอร์ชันที่ 4 ยังเพิ่มการรองรับคำสั่งต่างๆ เช่น การจับภาพหน้าจอ การคลิกและการปัด การคัดลอกและวางไฟล์และการแสดงหน้าจอซ้อนทับได้ตามต้องการ รุ่นนี้ยังมีการปรับโครงสร้างโค้ดที่สำคัญในกลไกการขโมยคุกกี้ ซึ่งขณะนี้กำหนดเป้าหมายไปที่ Gmail, GPay และ Google Password Manager แต่ในเวอร์ชันที่ 5 ยังไม่มีการเผยแพร่อย่างกว้างขวาง และโมดูล VNC หายไปจากตัวอย่างแรกๆ ดังนั้นจึงมีแนวโน้มว่าเวอร์ชันนี้ยังอยู่ระหว่างการพัฒนา แม้จะอยู่ในรูปแบบปัจจุบันที่ยังไม่เสร็จก็ตาม SOVA v5 ก็พร้อมสำหรับการใช้งาน ตามข้อมูลของ Cleafy ดังนั้นผู้ใช้ Android ทุกคนจึงควรระมัดระวัง สิ่งนี้ทำให้ SOVA เป็นภัยคุกคามต่อความรุนแรงที่เพิ่มขึ้น เนื่องจากโทรจันธนาคารกำลังตั้งตัวเองให้เป็นหนึ่งในผู้บุกเบิกแรนซัมแวร์บนมือถือ

ที่มาของข่าว : https://www.bleepingcomputer.com/news/security/sova-malware-adds-ransomware-feature-to-encrypt-android-devices/